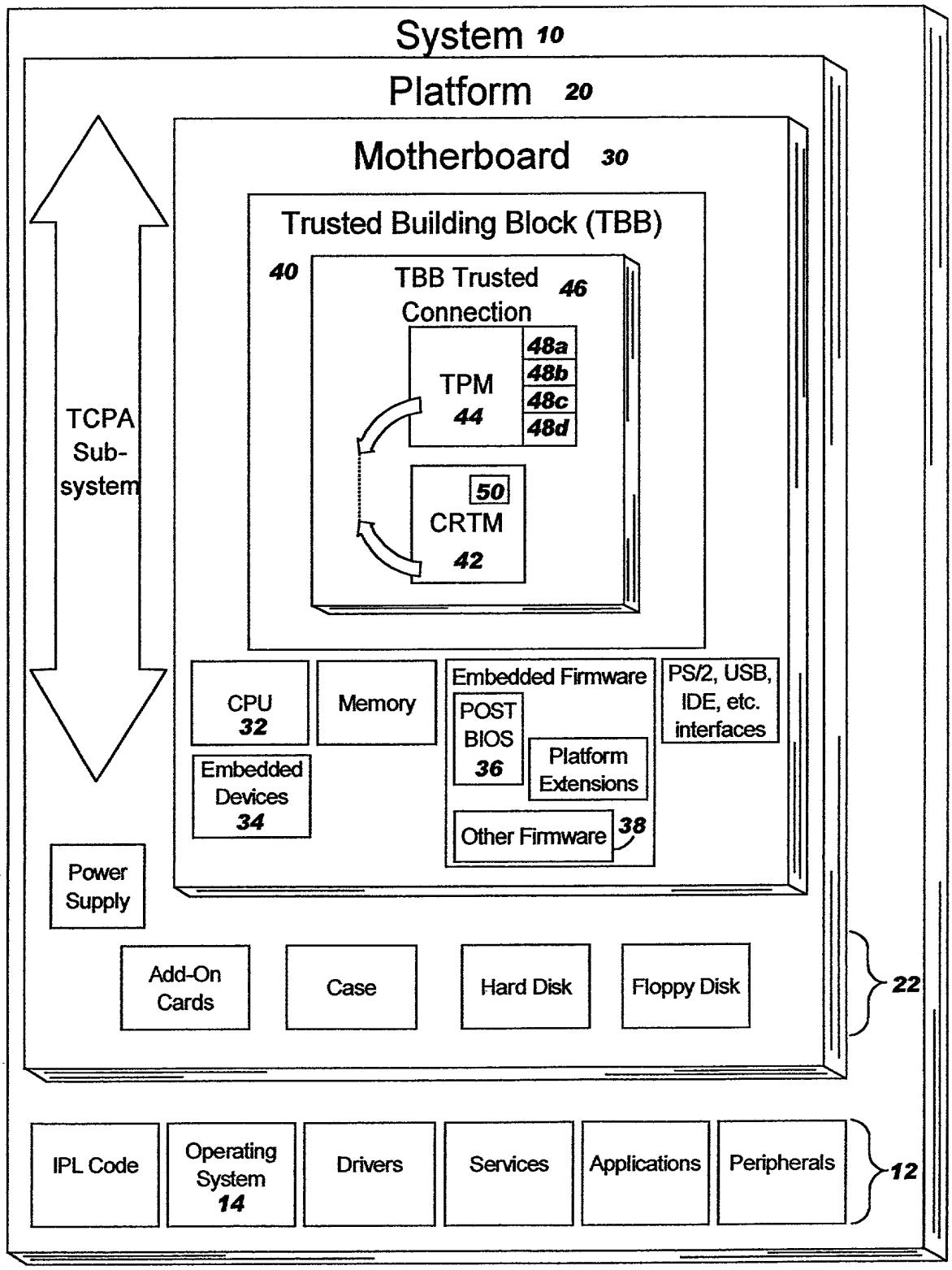
FIG. 1


System 10
Platform 20
Motherboard 30
Trusted Building Block (TBB)
40
TBB Trusted Connection 46
TPM 44
48a
48b
48c
48d
50
CRTM 42
TCPA Sub-system
CPU 32
Memory
Embedded Firmware
POST BIOS 36
Platform Extensions
Other Firmware 38
PS/2, USB, IDE, etc. interfaces
Embedded Devices 34
Power Supply
Add-On Cards
Case
Hard Disk
Floppy Disk
22
IPL Code
Operating System 14
Drivers
Services
Applications
Peripherals
12

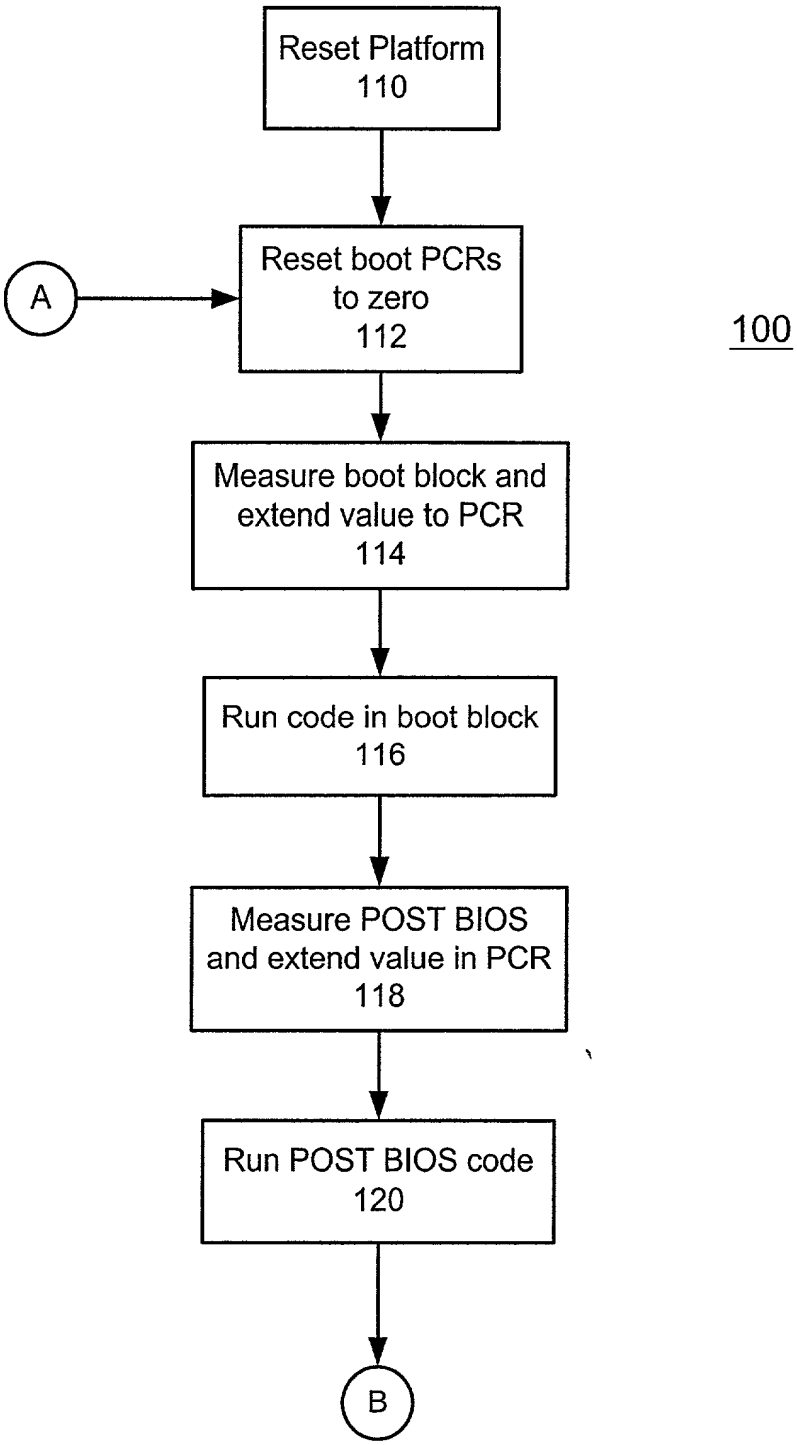

Reset Platform
110
A
Reset boot PCRs
to zero
112
100
Measure boot block and
extend value to PCR
114
Run code in boot block
116
Measure POST BIOS
and extend value in PCR
118
Run POST BIOS code
120
B

FIG. 2A

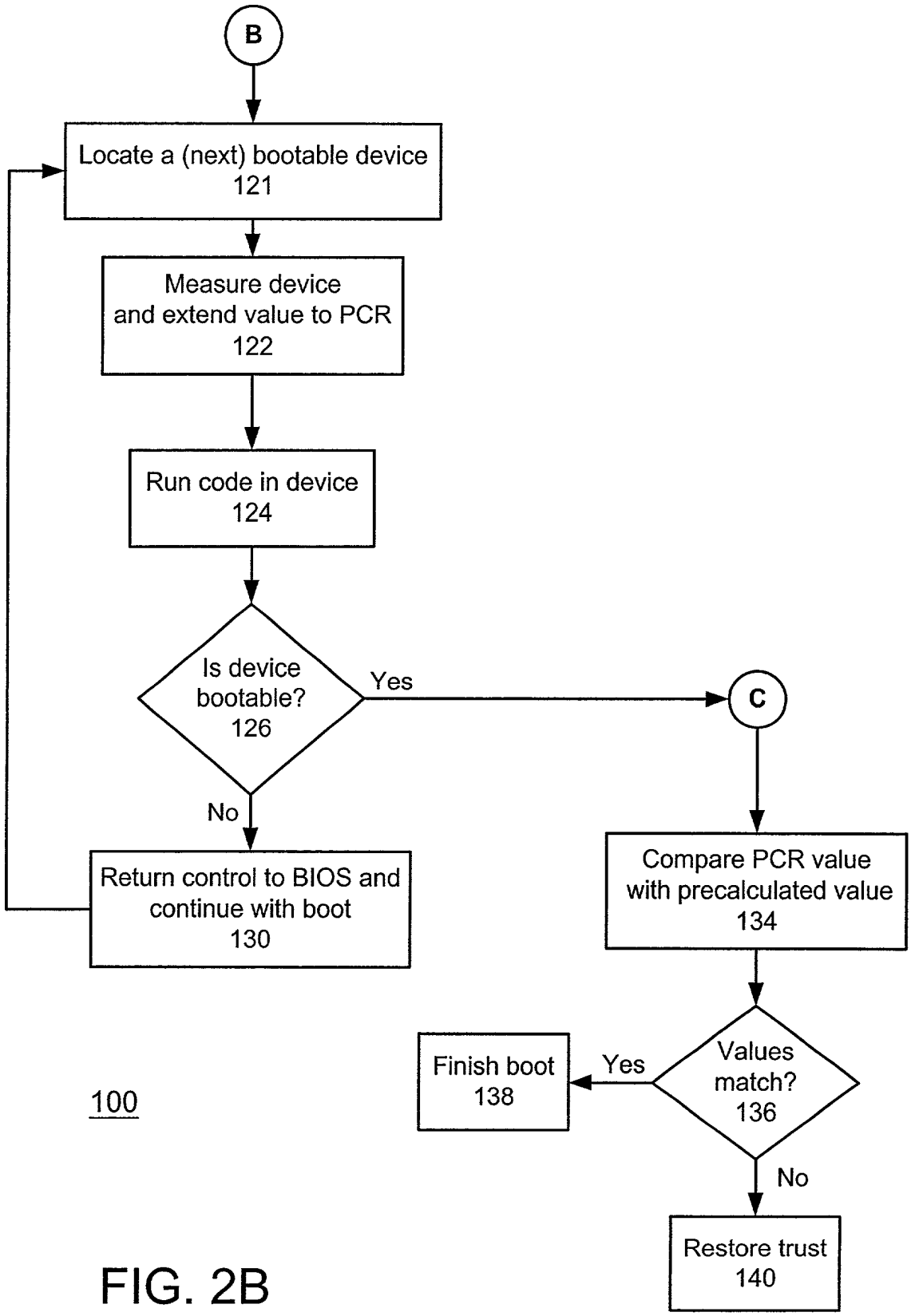

B
Locate a (next) bootable device
121
Measure device
and extend value to PCR
122
Run code in device
124
Is device
bootable?
126
Yes
No
C
Return control to BIOS and
continue with boot
130
Compare PCR value
with precalculated value
134
Values
match?
136
Yes
Finish boot
138
No
Restore trust
140
100

FIG. 2B

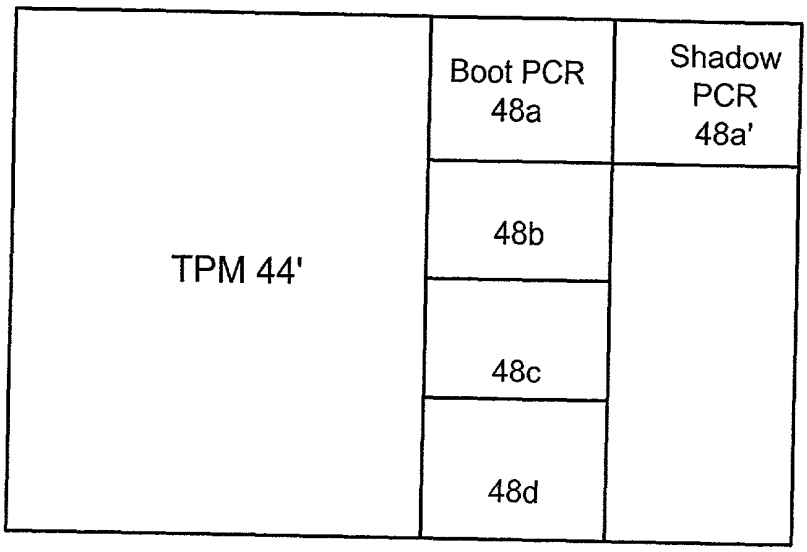


FIG. 3

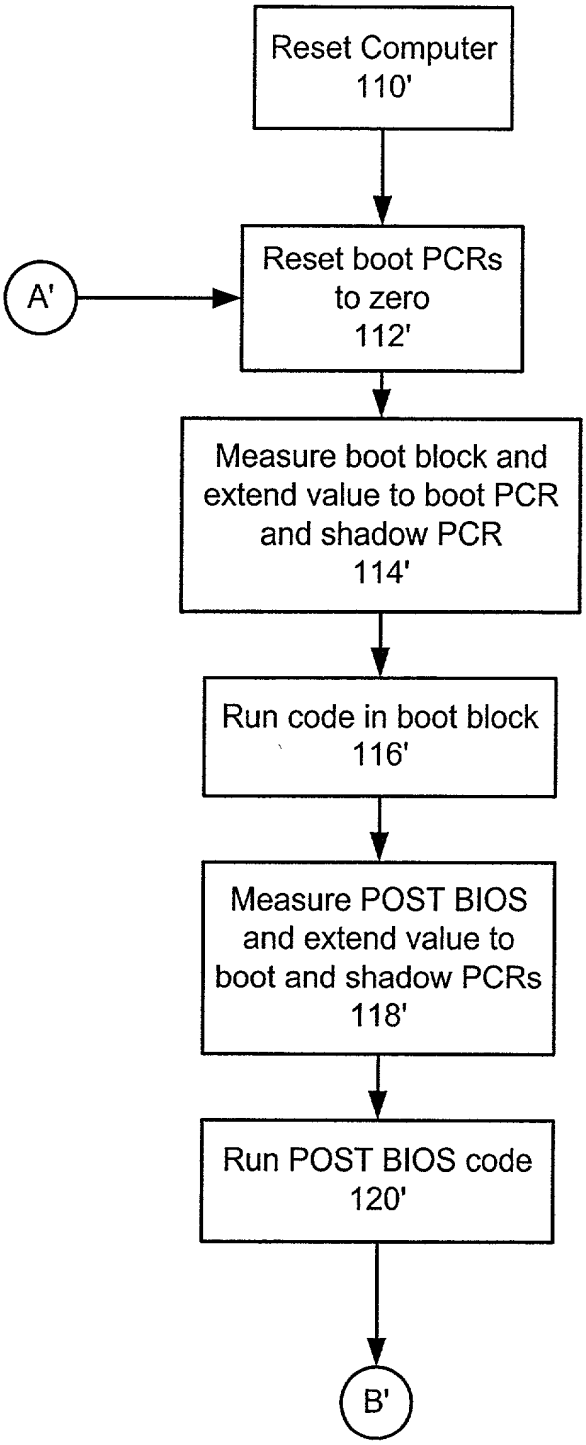

Reset Computer
110'
A'
Reset boot PCRs
to zero
112'
Measure boot block and
extend value to boot PCR
and shadow PCR
114'
Run code in boot block
116'
Measure POST BIOS
and extend value to
boot and shadow PCRs
118'
Run POST BIOS code
120'
B'

FIG. 3A

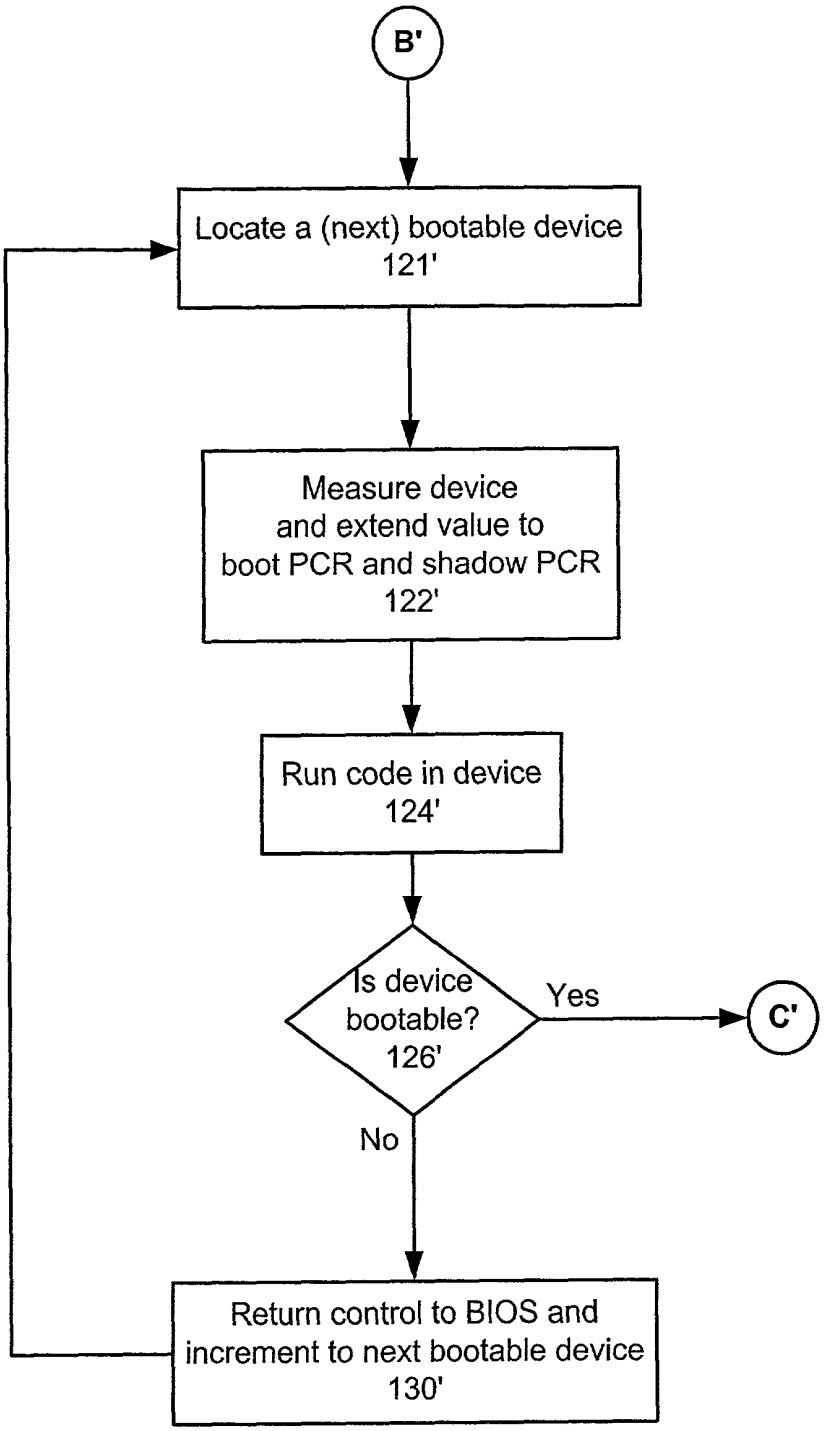

B'
Locate a (next) bootable device
121'
Measure device
and extend value to
boot PCR and shadow PCR
122'
Run code in device
124'
Is device
bootable?
126'
Yes
C'
No
Return control to BIOS and
increment to next bootable device
130'

FIG. 3B

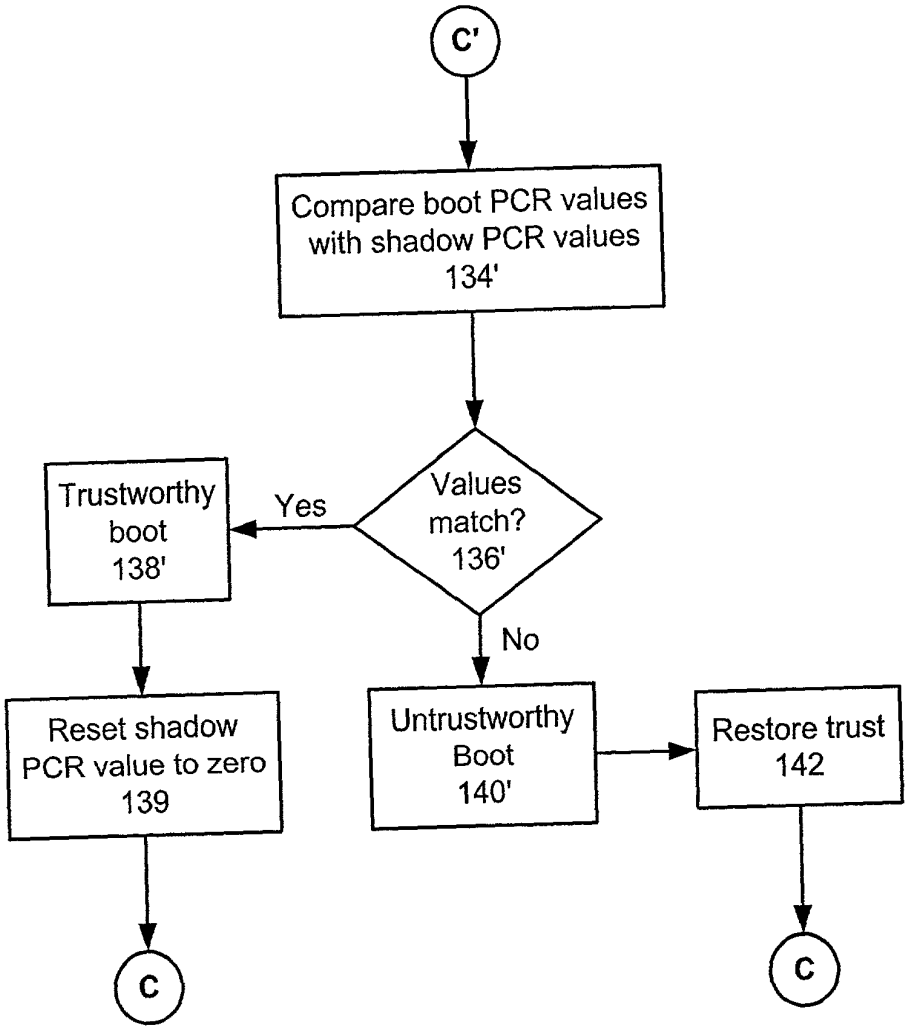

C'
Compare boot PCR values with shadow PCR values 134'
Values match? 136'
Yes
Trustworthy boot 138'
No
Untrustworthy Boot 140'
Restore trust 142
Reset shadow PCR value to zero 139
C
C

FIG. 3C